

Attorney Docket No. RSW920010221US1 (5577-357)

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Brabson et al.
Serial No.: 10/007,446
Filed: December 5, 2001
For: *Policy-Driven Kernel Based Security Implementation*


Confirmation No.: 3354
Examiner: Kristin D. Sandoval
Group Art Unit: 2132

Date: August 9, 2006

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATION OF TRANSMISSION

I hereby certify that this correspondence is being transmitted electronically to the U.S. Patent and Trademark Office on August 9, 2006.


Traci A. Brown

APPELLANTS' BRIEF ON APPEAL UNDER 37 C.F.R. §41.37

Sir:

This Appeal Brief is filed pursuant to the "Notice of Appeal to the Board of Patent Appeals and Interferences" filed June 22, 2006.

Real Party In Interest

The real party in interest is assignee International Business Machines, Inc., Armonk, New York.

Related Appeals and Interferences

Appellants are aware of no appeals or interferences that would be affected by the present appeal.

Status of Claims

Appellants appeal the final rejection of Claims 1, 2, and 4-18, which as of the filing date of this Brief remain under consideration. The claims at issue as included in Appellants' response to the final Office Action of March 23, 2006 are attached hereto as Appendix A.

Status of Amendments

Two responses have been filed in the present case: An "Amendment" was filed December 21, 2005 in response to an Office Action mailed October 5, 2005 (hereinafter "First Action"). An "Amendment After Final" was filed May 17, 2006 in response to a final Office Action mailed March 23, 2006 (hereinafter "Final Action"). Claim 3 was cancelled in the Amendment After Final. The amendments presented in the Amendment After Final were entered, but the rejections of Claims 1, 2 and 4-18 were maintained as indicated in an Advisory Action mailed June 8, 2006 (hereinafter "Advisory Action"). Therefore, Claims 1, 2 and 4-18, as amended, remain for consideration on the present appeal.

Summary of Claimed Subject Matter

Appellants appeal the final rejection of Independent Claims 1, 17 and 18. Independent Claim 1 is directed to a method of improving security processing in a computing network. The method includes providing security processing in an operating system kernel (TCP Layer of Fig. 2C; Specification, page 12, lines 3-5). An application program that makes use of the operating system kernel during execution is provided (210, 220 of Fig. 2C), and security policy information that is usable for more than one executing application program is provided (Specification, page 15, line 11 to page 16, line 6). The application program is executed (Block 345 of Fig. 3; Specification, page 26, lines 11-12), and at least one communication of the executing application program is selectably encrypted using the security processing provided in the operating system kernel, under conditions specified by the security policy information (Blocks 360, 315 and 320 of Fig. 3; Specification, page 16, line 1 to page 17, line 4; Specification, page 24, lines 10-13; Specification, page 26, line 11 through page 27, line 5).

In addition to providing security processing to applications that are not security enabled, this method promotes uniform treatment of security processing throughout an enterprise, as a consistent security policy can be applied to communications of multiple applications. In addition, this approach removes the need for applications to negotiate security processing and provides a system administrator the ability to manage security processing at a detailed level.

Independent Claim 17 is directed to a system for improving security processing in a computing network. The system includes means for performing security processing in an operating system kernel (TCP Layer of Fig. 2C; Specification, page 12, lines 3-5), and security policy information that is usable for more than one executing application program specifying conditions under which the means for performing security processing is to be activated (Specification, page 15, line 11 to page 16, line 6). The system further includes means for selectably encrypting at least one communication of an executing application program according to the conditions specified by the security policy information, using the means for performing security processing in an operating system kernel (TCP Layer of Fig. 2C; Specification, page 16, line 1 to page 17, line 4).

Independent Claim 18 is directed to a computer program product for improving security processing in a computing network. The computer program product includes a computer usable medium having computer readable program code embodied therein. The computer usable medium includes computer-readable program code configured to perform security processing in an operating system kernel (TCP Layer of Fig. 2C; Specification, page 12, lines 3-5), and computer-readable program code configured to access security policy information that is usable for more than one executing application program (TCP Layer of Fig. 2C; Specification, page 12, lines 3-5), the security policy information specifying at least one condition under which the computer-readable program code configured to perform security processing is to be activated (Specification, page 15, line 1 to page 16, line 6). The computer usable medium further includes computer-readable program code configured to execute an application program which makes use of the operating system kernel during execution (Block 345 of Fig. 3; Specification, page 26, lines 11-12), and computer-readable program code configured to selectably encrypt at least one communication of the executing application program according to the conditions specified by the security policy information, using the computer-readable program code configured to perform security processing (Blocks 360, 315 and 320 of Fig. 3; Specification, page 16, lines 1-16; Specification, page 24, lines 10-13; Specification, page 26, line 11 through page 27, line 5).

Grounds of Rejection to be Reviewed on Appeal

In the Final Action, Independent Claims 1, 17 and 18 were rejected under 35 USC § 102(b) as anticipated by U.S. Patent No. 5,029,206 to Marino et al. (hereinafter "Marino"), while Claim 3 was rejected under 35 U.S.C. §103(a) as being obvious over Marino in view of U.S. Patent No. 6,131,163 to Wiegel (hereinafter "Wiegel"). In the Amendment After Final, Independent Claims 1, 17 and 18 were amended to include the recitations of Claim 3, which was cancelled. The Advisory Action indicated that the amendments would be entered, but that rejection of Claim 3 under 35 U.S.C. §103(a) would be applied to Independent Claims 1, 17 and 18, as amended. Accordingly, Independent Claims 1, 17 and 18 presently stand rejected under 35 U.S.C. §103(a) as being obvious over Marino in view of Wiegel.

Argument

I. Introduction to 35 U.S.C. §103 Analysis

Claims 1, 17 and 18 stand rejected as obvious under 35 U.S.C. §103(a). A determination under §103 that an invention would have been obvious to someone of ordinary skill in the art is a conclusion of law based on fact. *Panduit Corp. v. Dennison Mfg. Co.* 810 F.2d 1593, 1 U.S.P.Q.2d 1593 (Fed. Cir. 1987), *cert. denied*, 107 S.Ct. 2187. After the involved facts are determined, the decision maker must then make the legal determination of whether the claimed invention as a whole would have been obvious to a person having ordinary skill in the art at the time the invention was unknown, and just before it was made. *Id.* at 1596. The United States Patent and Trademark Office (USPTO) has the initial burden under §103 to establish a *prima facie* case of obviousness. *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q.2d 1596, 1598 (Fed. Cir. 1988).

To establish a *prima facie* case of obviousness, the prior art reference or references when combined must teach or suggest *all* the recitations of the claims, and there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. M.P.E.P. §2143. The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. M.P.E.P. §2143.01, citing *In re Mills*, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed.

Cir. 1990). As emphasized by the Court of Appeals for the Federal Circuit, to support combining references, evidence of a suggestion, teaching, or motivation to combine must be **clear and particular**, and this requirement for clear and particular evidence is not met by broad and conclusory statements about the teachings of references. *In re Dembiczak*, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999). In another decision, the Court of Appeals for the Federal Circuit has stated that, to support combining or modifying references, there must be **particular** evidence from the prior art as to the reason the skilled artisan, with no knowledge of the claimed invention, would have selected these components for combination in the manner claimed. *In re Kotzab*, 55 U.S.P.Q.2d 1313, 1317 (Fed. Cir. 2000).

Appellants respectfully submit that the pending claims are patentable over the cited references for at least the reason that neither the cited references nor the combination thereof disclose or suggest each of the recitations of the claims. The patentability of the pending claims is discussed in detail hereinafter.

II. Independent Claims 1, 17 and 18 are Patentable over Marino and Wiegel

Claim 1, as amended, recites as follows:

1. A method of improving security processing in a computing network, comprising:
 - providing security processing in an operating system kernel;
 - providing an application program which makes use of the operating system kernel during execution;
 - providing security policy information that is usable for more than one executing application program;
 - executing the application program; and
 - selectably encrypting at least one communication of the executing application program using the provided security processing in the operating system kernel, under conditions specified by the security policy information (emphasis added).

Neither Marino nor Wiegel, alone or in combination, discloses selectably encrypting at least one communication of an executing application program using security processing provided in an operating system kernel, under conditions specified by security policy information that is usable for more than one executing application program, as recited in Claim 1.

Marino discloses a security kernel for providing security functions in a system including a subsystem (the "red" subsystem) that exchanges plain text data and a subsystem (the "black" subsystem") that transmits cypher text data. See Marino, Abstract. The security kernel of Marino includes a Key Management User Agent (KMUA), which is a module that has, as one of its functions, establishing cryptographic associations between network encryption devices. Marino, column 5, lines 52-54. The system of Marino relies on information provided to the security processing modules such as the KMUA by the application programs themselves. As stated in Marino:

An application program of the red processing side initiates a request to the KMUA as depicted by transfer 101. The application software passes along to the KMUA 40 a number of parameters. These parameters include the title or name of the remote subsystem with which the cryptographic association is to be established. Next, the red side application software indicates via a parameter what cryptographic algorithm is to be selected for the data encryption and decryption. Further parameters passed by the application software to KMUA 40 include options and crypto modes. These modes indicate such parameters as one-way or two-way traffic encryption keys or other considerations related to a specific algorithm to be used.

Marino, column 7, lines 36-50. Accordingly, in the system of Marino, when a secure communication session is to be established, security information is passed from the application program to the security kernel. This is in direct contrast to Claim 1, which recites selectably encrypting a communication of an executing application program using security processing in the operating system kernel, under conditions specified by security policy information that is usable for more than one executing application program. Since the security processing of Marino is performed in response to security parameters passed by individual programs, the security processing of Marino is not performed under conditions specified by security policy information that is usable for more than one executing application program. Moreover, there is no indication in Marino that the parameters passed by an application to the security modules described therein are usable for more than one application program.

The Final Action stated that Wiegel teaches a method wherein the security policy information is usable for more than one executing application program. Final Action, p. 3. Wiegel discloses a system for a network gateway that provides computer data security using a protocol stack proxy. See Wiegel, Abstract. In particular, Wiegel describes a system for

detecting whether requests to a system are accurate, valid and come from an authorized system. Wiegel, column 1, lines 47-50. That is, Wiegel is concerned with repelling unauthorized requests and malicious attacks originating outside a computer system. *See* Wiegel, column 1, lines 51-55.

Wiegel describes the use of a "policy tree" that is a representation of an abstract security policy that can instruct the system to accept or reject a data packet based upon criteria relating to the data packet. Wiegel, column 9, lines 38-41. Thus, the "policy tree" of Wiegel does not correspond to "security policy information" as recited in Claim 1 that provides conditions for selectably encrypting a communication of an application program. Thus, even if Wiegel and Marino were combined, the resulting system would not provide a system that selectably encrypts a communication of an executing application program using security processing provided in the operating system kernel, under conditions specified by security policy information that is usable for more than one application program, as recited in Claim 1.

The Advisory Action states that the combination of Marino and Wiegel would produce a security system that protects a system and its services from attacks outside a network at the kernel level using its security policies. Advisory Action, p. 2. However, the combined system hypothesized in the Advisory Action is not the subject matter to which Claim 1 is directed. That is, Claim 1 is directed to securing communications of an application program, not securing a system against attacks outside a network. Thus, even if Marino and Wiegel were combined, it would simply provide the system of Marino with port-level security processing as described in Wiegel, and would not suggest a system that selectably encrypts a communication of an executing application program using provided security processing in the operating system kernel, under conditions specified by security policy information that is usable by more than one application program, as recited in Claim 1.

Accordingly, even if combined, Marino and Wiegel do not teach or suggest each and every recitation of Claim 1. Claim 17 recites means for selectably encrypting at least one communication of an executing application program according to conditions specified by security policy information that is usable for more than one executing application program. Similarly, Claim 18 recites computer-readable program code configured to selectably encrypt at least one communication of an executing application program according to conditions specified

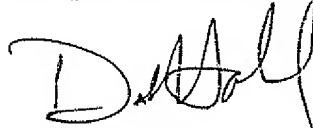
by security policy information that is usable for more than one executing application program. Thus, the foregoing conclusion applies equally to Claims 17 and 18.

For at least the foregoing reasons, Appellants respectfully submit that independent Claims 1, 17 and 18 are patentable over Marino in view of Wiegel and that dependent Claims 2 and 4-16 are patentable at least by virtue of their depending from an allowable claim. Accordingly, Appellants respectfully request that the rejection of independent Claims 1, 17 and 18 be reversed based on the failure of the Examiner to establish a prima facie case of obviousness under 35 U.S.C. §103 for at least these reasons.

III. Conclusion

In summary, Appellants respectfully submit that, with respect to Claims 1, 17 and 18, the cited references do not teach or suggest all of the recitations of the claims, either alone or in combination. Accordingly, Appellants respectfully request reversal of the rejection of Claims 1, 17 and 18 based on the cited references.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'D. Hall', with a stylized flourish at the end.

David C. Hall
Registration No. 38,904

Myers Bigel Sibley & Sajovec, P.A.
P. O. Box 37428
Raleigh, North Carolina 27627
Telephone: (919) 854-1400
Facsimile: (919) 854-1401
Customer No. 46589

APPENDIX A

1. (Previously Amended) A method of improving security processing in a computing network, comprising:

providing security processing in an operating system kernel;

providing an application program which makes use of the operating system kernel during execution;

providing security policy information that is usable for more than one executing application program;

executing the application program; and

selectably encrypting at least one communication of the executing application program using the provided security processing in the operating system kernel, under conditions specified by the security policy information.

2. (Original) The method according to claim 1, wherein the security policy information is stored in a security repository.

3. (Cancelled)

4. (Previously Amended) The method according to claim 1, wherein the conditions comprise network addresses.

5. (Previously Amended) The method according to claim 4, wherein the network addresses specify at least one of server addresses and destination addresses.

6. (Previously Amended) The method according to claim 4, wherein the network addresses comprise at least one of ranges of source addresses and ranges of destination addresses.

7. (Previously Amended) The method according to claim 1, wherein the conditions comprise at least one of port numbers and port number ranges.

8. (Previously Amended) The method according to claim 1, wherein the conditions comprise at least one job name.

9. (Previously Amended) The method according to claim 1, wherein the conditions comprise at least one client identifier.

10. (Previously Amended) The method according to claim 1, further comprising checking the security policy information when the executing application program establishes a connection, and wherein the communications on that connection are encrypted.

11. (Previously Amended) The method according to claim 1, wherein communications from the executing application program are encrypted even though the provided application program has no code for security processing.

12. (Previously Amended) The method according to claim 1, wherein the provided application program invokes at least one security directive, and further comprising executing, during execution of the provided application program, at least one of the invoked security directives.

13. (Previously Amended) The method according to claim 1, wherein, when a result of evaluating the security policy information so indicates, communications on only some sockets of a port are encrypted.

14. (Original) The method according to claim 1, wherein the provided security processing operates in a Transmission Control Protocol layer of the operating system kernel.

15. (Original) The method according to claim 1, wherein the provided security processing implements Secure Sockets Layer.

16. (Previously Amended) The method according to claim 1, wherein the provided security processing implements Transport Layer Security.

17. (Previously Amended) A system for improving security processing in a computing network, comprising:

- means for performing security processing in an operating system kernel;

- security policy information that is usable for more than one executing application program specifying at least one condition under which the means for performing security processing is to be activated;

- means for executing an application program which makes use of the operating system kernel during execution; and

- means for selectably encrypting, according to the conditions specified by the security policy information, at least one communication of the executing application program using the means for performing security processing.

18. (Previously Amended) A computer program product for improving security processing in a computing network, the computer program product comprising:

- a computer usable medium having computer readable program code embodied therein, the computer usable medium comprising:

- computer-readable program code configured to perform security processing in an operating system kernel;

- computer-readable program code configured to access security policy information that is usable for more than one executing application program, the security policy information specifying at least one condition under which the computer-readable program code configured to perform security processing is to be activated;

- computer-readable program code configured to execute an application program which makes use of the operating system kernel during execution; and

computer-readable program code configured to selectably encrypt, according to the conditions specified by the security policy information, at least one communication of the executing application program using the computer-readable program code configured to perform security processing.

In re: Brabson et al.
Serial No.: 10/007,446
Filed: December 5, 2001
Page 13

APPENDIX B – EVIDENCE APPENDIX

None

In re: Brabson et al.
Serial No.: 10/007,446
Filed: December 5, 2001
Page 14

APPENDIX C – RELATED PROCEEDINGS APPENDIX

None.